

## Appendix A

### Privacy Breach Protocol and Privacy Complaint Protocol for Treasury Board, Executive Council Office, Office of Policy and Priorities, and the Chief Information Office (“the Offices”)

*A Privacy Breach may be discovered through a variety of means. It may be uncovered unexpectedly in the course of normal business activity. It might be very obvious as soon as it happens. Or there could be a complaint from someone whose information was involved, or from a third party. Regardless, there must be a clear set of instructions on how to proceed once a privacy breach is suspected or discovered.*

*The first part of this protocol is for responding to a breach or suspicion of a breach, however it occurred. The second part is a protocol for responding to an actual complaint about an alleged privacy breach, which requires additional steps to be considered.*

## PART I

### Privacy Breach Protocol for “the Offices”

#### 1. Identify the privacy breach.

*Once the potential of a privacy breach has been identified, establish the date, time, location, length, type and extent of the breach.*

#### 2. Immediate remedial action.

*Identify what action is to be taken to contain/stop the breach. For consideration:*

- ▶ *Were hard copies of any faxed personal information retrieved or was there confirmation that the recipient(s) securely disposed of the fax?*
- ▶ *Was the GroupWise recipient(s) who had opened the email contacted to request the email be deleted and hard copies securely destroyed?*
- ▶ *Regarding a recipient(s) not on the GroupWise system, did you contact the recipient(s) to request deletion of the email and secure disposal of any hard copies?*
- ▶ *Will the breach allow access to any other personal information, and if so, were steps taken to avoid this potential additional breach?*
- ▶ *If an electronic device and paper records containing personal information was stolen, did you immediately contact security (if within a public body facility) or the police (if outside a public body facility)?*

### **3. Internal notification.**

*Provide instructions on who needs to be notified internal to your organization.*

*NOTE: In all cases, notify your supervisor and the FOIPOP Administrator, who will consult with the Communications Advisor. Also recommended:*

- ▶ *If the breach involves a website, the IT Director will be contacted or if there is a danger to an individual or the public, contact CITO.*
- ▶ *If the breach is serious or could be potentially serious, the Deputy Minister and Legal Counsel need to be contacted.*

### **4. Investigation and documentation.**

*Determine the detail of what/whose personal information is involved, and what is the extent/scope of the breach. Example questions:*

- ▶ *Were the immediate remedial actions effective?*
- ▶ *Is there enough documented evidence about the incident to determine the series of events that led to the breach?*

### **5. External documentation.**

*When personal privacy is breached, it is necessary to determine which stakeholders (e.g. public bodies or municipalities, general public, individuals, etc.) should be notified, under what circumstances, and when. Outline external notification requirements. For consideration:*

*After the FOIPOP Administrator consults with the Deputy Minister and Legal Counsel, one or more of the following may need to be notified:*

- ▶ *Individual(s) whose privacy has been breached*
- ▶ *Chair of BTAC / Chief Information Officer, Province of Nova Scotia*
- ▶ *Communications Nova Scotia (through your Communications Director)*
- ▶ *Security Authority, and/or*
- ▶ *Other individuals who may have been affected by the breach.*

## **6. Follow-up and long-term remedial action**

*Determine what follow-up and long-term remedial action there will be to prevent the breach from occurring again (e.g. analysis of incident to identify future preventive measures). Example questions include:*

- ▶ *Was the privacy breach protocol followed?*
- ▶ *Are new or amended policies, procedures and/or training required to prevent re-occurrence of the breach?*
- ▶ *What plans have to be developed to lessen the likelihood or eliminate the possibility of another breach?*

## PART 2

### Privacy Complaint Protocol for “the Offices”

#### 1. Receive and document the complaint.

*When a complaint is received, discuss the details of the alleged breach with the complainant and document what the complainant believes has happened. This is a critical first step and should be completed in writing so that it can form part of the record of “the Offices” response to the complaint. It is recommended that a consistent format be used for this purpose. The Information Access and Privacy Office (Justice) will be developing a template for use by government entities in the near future. In the meantime, the following structure is recommended.*

#### 2. Follow Steps 2 through 6 of the Privacy Breach Protocol.

*At this point, all of the steps required for a self-identified or suspected privacy breach are the same as described in the previous template. Containment, internal and external notifications, full investigation and follow-up are all required.*

#### 3. Complainant communication.

*A complaint obviously differs from an internal discovery to the extent that there is an external complainant. Communication throughout the process and at the end of the process with the complainant(s) is a unique requirement in this regard.*

*Governed by the complexity of the breach scenario and the duration of the ensuing investigation, the following steps should be incorporated into “the Offices” complaint procedure:*

- 3.1 *Send written acknowledgment to the complainant, re-stating the details presented by the complainant to “the Offices”, and an indication of who is accountable internally for the investigation (first formal correspondence).*
- 3.2 *Send written update of progress of the investigation (stage of investigation, follow-up activities, expected or updated time frames, etc.). This step should be triggered by the time that has elapsed since initial acknowledgment of the complaint. A written update is required no later than two months from the acknowledgment. Updates continue on a schedule set out in “the Offices” procedure.*

- 3.3 *Generate a report of the results of the investigation. At a minimum, the report is to include:*
- verification of the breach*
  - mitigating activities*
  - other follow-up activities*
- 3.4 *Share the de-identified details of the breach investigation with the Information Access and Privacy Office at Justice for incorporation into training and communication (optional)*